

日本国特許庁
JAPAN PATENT OFFICE

04.11.2004

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日 2004年 2月10日
Date of Application:

REC'D 23 DEC 2004

WIPO PCT

出願番号 特願2004-034172
Application Number:
[ST. 10/C] : [JP 2004-034172]

出願人 エヌ・ティ・ティ・コミュニケーションズ株式会社
Applicant(s):

PRIORITY
DOCUMENT
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH RULE 17.1(a) OR (b)

2004年12月13日

特許庁長官
Commissioner,
Japan Patent Office

小川

洋

BEST AVAILABLE COPY

【書類名】 特許願
【整理番号】 GLN00468
【提出日】 平成16年 2月10日
【あて先】 特許庁長官 今井 康夫 殿
【国際特許分類】 G06F 17/00
 H04L 12/22

【発明者】
【住所又は居所】 東京都千代田区内幸町一丁目1番6号 エヌ・ティ・ティ・コミュニケーションズ株式会社内
【氏名】 深田 聰

【発明者】
【住所又は居所】 東京都千代田区内幸町一丁目1番6号 エヌ・ティ・ティ・コミュニケーションズ株式会社内
【氏名】 山崎 俊之

【発明者】
【住所又は居所】 東京都千代田区内幸町一丁目1番6号 エヌ・ティ・ティ・コミュニケーションズ株式会社内
【氏名】 白崎 泰弘

【発明者】
【住所又は居所】 東京都千代田区内幸町一丁目1番6号 エヌ・ティ・ティ・コミュニケーションズ株式会社内
【氏名】 齊藤 允

【発明者】
【住所又は居所】 東京都千代田区内幸町一丁目1番6号 エヌ・ティ・ティ・コミュニケーションズ株式会社内
【氏名】 徳永 治
【特許出願人】
【識別番号】 399035766
【氏名又は名称】 エヌ・ティ・ティ・コミュニケーションズ株式会社

【代理人】
【識別番号】 100070150
【弁理士】
【氏名又は名称】 伊東 忠彦

【先の出願に基づく優先権主張】
【出願番号】 特願2003-374880
【出願日】 平成15年11月 4日

【手数料の表示】
【予納台帳番号】 002989
【納付金額】 21,000円

【提出物件の目録】
【物件名】 特許請求の範囲 1
【物件名】 明細書 1
【物件名】 図面 1
【物件名】 要約書 1
【包括委任状番号】 0113902

【書類名】特許請求の範囲**【請求項 1】**

ネットワークに接続された第1の端末と第2の端末との間で暗号化通信チャネルを確立するための方法であって、

前記ネットワークに接続されたセッション管理装置と第1の端末との間で相互認証を行い、セッション管理装置と第1の端末との間で第1の暗号化通信チャネルを確立するステップと、

セッション管理装置と第2の端末との間で相互認証を行い、セッション管理装置と第2の端末との間で第2の暗号化通信チャネルを確立するステップと、

第1の暗号化通信チャネルと第2の暗号化通信チャネルとを介して第1の端末と第2の端末との間で鍵情報を交換するステップと

を有することを特徴とする方法。

【請求項 2】

ネットワークに接続された第1の端末と第2の端末との間で暗号化通信チャネルを確立するための方法であって、

前記ネットワークに接続されたセッション管理装置と第1の端末との間で暗号化通信のための鍵情報を交換し、セッション管理装置と第1の端末が相互に認証を行い、セッション管理装置と第1の端末との間で第1の暗号化通信チャネルを確立するステップと、

セッション管理装置と第2の端末との間で暗号化通信のための鍵情報を交換し、セッション管理装置と第2の端末が相互に認証を行い、セッション管理装置と第2の端末との間で第2の暗号化通信チャネルを確立するステップと、

第1の端末が、第1の端末と第2の端末との間の暗号化通信のための鍵情報を含む第2の端末への接続要求メッセージを第1の暗号化通信チャネルを介してセッション管理装置に送信し、セッション管理装置が、その接続要求メッセージを第2の暗号化通信チャネルを介して第2の端末に送信するステップと、

第2の端末が、前記接続要求メッセージへの応答として、第1の端末と第2の端末との間の暗号化通信のための鍵情報を含む応答メッセージを第2の暗号化通信チャネルを介してセッション管理装置に送信し、セッション管理装置が、その応答メッセージを第1の暗号化通信チャネルを介して第1の端末に送信するステップと

を有することを特徴とする方法。

【請求項 3】

第1の端末とセッション管理装置との間のメッセージ通信、及び第2の端末とセッション管理装置との間のメッセージ通信をSIPに基づき行う請求項1又は2に記載の方法。

【請求項 4】

第1の端末が、前記第1の暗号化通信チャネルを介して、第1の端末の名前とアドレスをセッション管理装置に登録するステップと、

第2の端末が、前記第2の暗号化通信チャネルを介して、第2の端末の名前とアドレスをセッション管理装置に登録するステップとを更に有し、

第1の端末から送信される前記接続要求メッセージは第2の端末の名前を含み、前記セッション管理装置は、当該名前から第2の端末のアドレスを取得し、当該アドレス宛に前記接続要求メッセージを送信する請求項2に記載の方法。

【請求項 5】

前記セッション管理装置は、端末間で接続を許可するか否かの情報を保持し、接続要求メッセージを受信した場合に、当該情報を参照して、接続要求元の端末が接続要求先の端末と接続することが許容されているか否かを判断し、許容されていない場合には、接続を拒否する請求項2に記載の方法。

【請求項 6】

前記第1の端末が第3の端末からのアクセスを受けた後に前記各ステップが実行され、前記各ステップの実行により確立された前記第1の端末と前記第2の端末との間の暗号化通信チャネルを介して、前記第1の端末が前記第2の端末からデータを受信し、当該データ

タを前記第3の端末に送信する請求項1又は2に記載の方法。

【請求項7】

前記第1の端末が第3の端末からのアクセスを受けた後に、前記第1の暗号化通信チャネル及び前記第2の暗号化通信チャネル確立のためのステップ以降の各ステップが実行され、当該各ステップの実行により確立された前記第1の端末と前記第2の端末との間の暗号化通信チャネルを介して、前記第1の端末が前記第2の端末からデータを受信し、当該データを前記第3の端末に送信する請求項1又は2に記載の方法。

【請求項8】

ネットワークに接続された第1の端末と第2の端末との間に暗号化通信チャネルを確立するための方法であって、

前記ネットワークに接続された公開鍵管理装置と第1の端末との間で暗号化通信のための鍵情報を交換し、公開鍵管理装置と第1の端末が相互に認証を行う暗号化通信チャネル確立ステップと、

第1の端末が秘密鍵と公開鍵を生成し、当該公開鍵を、前記暗号化通信チャネル確立ステップにより確立された公開鍵管理装置と第1の端末との間の暗号化通信チャネルを介して公開鍵管理装置に送信するステップと、

公開鍵管理装置が、受信した公開鍵の公開鍵証明書を生成し、当該公開鍵証明書を、公開鍵管理装置と第1の端末との間の前記暗号化通信チャネルを介して第1の端末に送信するステップと、

第1の端末が、第2の端末に当該公開鍵証明書を配布することにより、第1の端末と第2の端末との間で公開鍵を用いた暗号化通信チャネルを確立するステップと
を有することを特徴とする方法。

【請求項9】

前記公開鍵管理装置は、前記暗号化通信チャネル確立ステップを実行して第1の端末との間で前記暗号化通信チャネルを確立するサーバと、当該サーバに暗号化通信チャネルを介して接続された公開鍵証明書を生成・管理する機能を有する装置とからなる請求項8に記載の方法。

【請求項10】

第1の端末と公開鍵管理装置との間のメッセージ通信をSIPに基づき行う請求項8又は9に記載の方法。

【請求項11】

ネットワークに接続された第1の端末と第2の端末との間で暗号化通信チャネルを確立するための方法であって、

前記ネットワークに接続された公開鍵管理装置と第1の端末との間で暗号化通信のための鍵情報を交換し、公開鍵管理装置と第1の端末が相互に認証を行う第1の暗号化通信チャネル確立ステップと、

公開鍵管理装置と第2の端末との間で暗号化通信のための鍵情報を交換し、公開鍵管理装置と第2の端末が相互に認証を行う第2の暗号化通信チャネル確立ステップと、

第1の端末が秘密鍵と公開鍵を生成し、当該公開鍵を、前記第1の暗号化通信チャネル確立ステップにより確立された公開鍵管理装置と第1の端末との間の第1の暗号化通信チャネルを介して公開鍵管理装置に送信するステップと、

公開鍵管理装置は受信した公開鍵を記憶装置に格納し、第2の端末が、当該公開鍵を、前記第2の暗号化通信チャネル確立ステップにより確立された公開鍵管理装置と第2の端末との間の第2の暗号化通信チャネルを介して取得するステップと、

第1の端末と第2の端末との間で当該公開鍵を用いた暗号化通信チャネルを確立するステップと

を有することを特徴とする方法。

【請求項12】

前記公開鍵管理装置は、第1の端末との間、及び第2の端末との間で暗号化通信チャネルを確立する装置と、当該装置と暗号化通信チャネルを介して接続された公開鍵を管理す

る機能を有する装置とからなる請求項11に記載の方法。

【請求項13】

第1の端末と公開鍵管理装置との間のメッセージ通信、及び第2の端末と公開鍵管理装置との間のメッセージ通信をSIPに基づき行う請求項11又は12に記載の方法。

【請求項14】

ネットワークに接続された第1の端末と第2の端末との間に暗号化通信チャネルを確立するためのセッション管理装置であって、

第1の端末との間で暗号化通信のための鍵情報を交換し、第1の端末と相互に認証を行い、セッション管理装置と第1の端末との間で第1の暗号化通信チャネルを確立する手段と、

第2の端末との間で暗号化通信のための鍵情報を交換し、第2の端末と相互に認証を行い、セッション管理装置と第2の端末との間で第2の暗号化通信チャネルを確立する手段と、

第1の端末から、第1の端末と第2の端末との間の暗号化通信のための鍵情報を含む第2の端末への接続要求メッセージを第1の暗号化通信チャネルを介して受信し、その接続要求メッセージを第2の暗号化通信チャネルを介して第2の端末に送信する手段と、

第2の端末から、第1の端末と第2の端末との間の暗号化通信のための鍵情報を含む応答メッセージを第2の暗号化通信チャネルを介して受信し、その応答メッセージを第1の暗号化通信チャネルを介して第1の端末に送信する手段と

を有することを特徴とするセッション管理装置。

【請求項15】

第1の端末とセッション管理装置との間のメッセージ通信、及び第2の端末とセッション管理装置との間のメッセージ通信をSIPに基づき行う手段を有する請求項14に記載のセッション管理装置。

【請求項16】

前記第1の暗号化通信チャネルを介して第1の端末の名前とアドレスを受信し、記憶装置に登録する手段と、

前記第2の暗号化通信チャネルを介して第2の端末の名前とアドレスを受信し、記憶装置に登録する手段とを更に有し、

第1の端末から送信される前記接続要求メッセージは、第2の端末の名前を含み、前記セッション管理装置は、当該名前から第2の端末のアドレスを取得する名前解決手段を有する請求項14に記載のセッション管理装置。

【請求項17】

前記セッション管理装置は、端末間で接続を許可するか否かの情報を保持し、接続要求メッセージを受信した場合に、当該情報を参照して、接続要求元の端末が接続要求先の端末と接続することが許容されているか否かを判断し、許容されていない場合には、接続を拒否する手段を有する請求項14に記載のセッション管理装置。

【請求項18】

ネットワークに接続された第1の端末と第2の端末との間に暗号化通信チャネルを確立するために使用する公開鍵を管理する公開鍵管理装置であって、

第1の端末との間で暗号化通信のための鍵情報を交換し、第1の端末と相互に認証を行う暗号化通信チャネル確立手段と、

第1の端末から、前記暗号化通信チャネル確立手段により確立された公開鍵管理装置と第1の端末との間の暗号化通信チャネルを介して、第1の端末の公開鍵を受信する手段と

、受信した公開鍵の公開鍵証明書を生成し、当該公開鍵証明書を、公開鍵管理装置と第1の端末との間の前記暗号化通信チャネルを介して第1の端末に送信する手段とを有することを特徴とする公開鍵管理装置。

【請求項19】

前記公開鍵管理装置は、前記暗号化通信チャネル確立手段を有するサーバと、当該サー

バに暗号化通信チャネルを介して接続された公開鍵証明書を生成・管理する機能を有する装置とからなる請求項18に記載の公開鍵管理装置。

【請求項20】

第1の端末と公開鍵管理装置との間のメッセージ通信をSIPに基づき行う手段を有する請求項18又は19に記載の公開鍵管理装置。

【請求項21】

ネットワークに接続された第1の端末と第2の端末との間に暗号化通信チャネルを確立するために使用する公開鍵を管理する公開鍵管理装置であって、

第1の端末との間で暗号化通信のための鍵情報を交換し、第1の端末と相互に認証を行う第1の暗号化通信チャネル確立手段と、

第2の端末との間で暗号化通信のための鍵情報を交換し、第2の端末と相互に認証を行う第2の暗号化通信チャネル確立手段と、

第1の端末から、前記第1の暗号化通信チャネル確立手段により確立された公開鍵管理装置と第1の端末との間の第1の暗号化通信チャネルを介して、第1の端末の公開鍵を受信する手段と、

受信した公開鍵を記憶装置に格納する手段と、

前記第2の暗号化通信チャネル確立手段により確立された公開鍵管理装置と第2の端末との間の第2の暗号化通信チャネルを介して、第1の端末の公開鍵を第2の端末に送信する手段と

を有することを特徴とする公開鍵管理装置。

【請求項22】

前記公開鍵管理装置は、第1の端末との間、及び第2の端末との間で暗号化通信チャネルを確立する装置と、当該装置に暗号化通信チャネルを介して接続された公開鍵を管理する機能を有する装置とからなる請求項21に記載の公開鍵管理装置。

【請求項23】

第1の端末と公開鍵管理装置との間のメッセージ通信、及び第2の端末と公開鍵管理装置との間のメッセージ通信をSIPに基づき行う手段を有する請求項21又は22に記載の公開鍵管理装置。

【請求項24】

ネットワークに接続されたセッション管理装置を用いて第2の端末との間で暗号化通信チャネルを確立する端末であって、

ネットワークに接続されたセッション管理装置との間で暗号化通信のための鍵情報を交換し、セッション管理装置と相互に認証を行い、セッション管理装置との間で暗号化通信チャネルを確立する第1の暗号化通信チャネル確立手段と、

前記端末と前記第2の端末との間の暗号化通信のための鍵情報を含む前記第2の端末への接続要求メッセージを、前記暗号化通信チャネル確立手段により確立された暗号化通信の接続要求メッセージを、前記暗号化通信チャネル確立手段により確立された暗号化通信チャネルを介してセッション管理装置に送信し、前記第2の端末から、セッション管理装置を介して、前記端末と前記第2の端末との間の暗号化通信のための鍵情報を含む応答メッセージを受信することにより、前記第2の端末との間で暗号化通信チャネルを確立する第2の暗号化通信チャネル確立手段と

を有することを特徴とする端末。

【請求項25】

前記端末は、第3の端末からのアクセスを受けた後に、前記端末と前記セッション管理装置との間の暗号化通信チャネルを確立するための処理と、前記端末と前記第2の端末との間の暗号化通信チャネルを確立するための処理を実行し、

前記端末と前記第2の端末との間の暗号化通信チャネルを介して前記第2の端末からデータを受信し、そのデータを前記第3の端末に送信する請求項24に記載の端末。

【請求項26】

前記端末は、第3の端末からのアクセスを受けた後に、前記端末と前記第2の端末との間の暗号化通信チャネルを確立するための処理を実行し、

前記端末と前記第2の端末との間の暗号化通信チャネルを介して前記第2の端末からデータを受信し、そのデータを前記第3の端末に送信する請求項24に記載の端末。

【請求項27】

前記端末は、前記第3の端末に対して許容されている少なくとも1つの接続先を示すテーブルを備え、前記第3の端末からのアクセスに応じて当該少なくとも1つの接続先の情報を前記第3の端末に送信し、前記第3の端末から接続先の指定を受ける請求項25又は26に記載の端末。

【請求項28】

コンピュータを、ネットワークに接続された第1の端末と第2の端末との間に暗号化通信チャネルを確立するためのセッション管理装置として機能させるプログラムであって、コンピュータを、

第1の端末との間で暗号化通信のための鍵情報を交換し、第1の端末と相互に認証を行い、セッション管理装置と第1の端末との間で第1の暗号化通信チャネルを確立する手段

、 第2の端末との間で暗号化通信のための鍵情報を交換し、第2の端末と相互に認証を行い、セッション管理装置と第2の端末との間で第2の暗号化通信チャネルを確立する手段

、 第1の端末から、第1の端末と第2の端末との間の暗号化通信のための鍵情報を含む第2の端末への接続要求メッセージを第1の暗号化通信チャネルを介して受信し、その接続要求メッセージを第2の暗号化通信チャネルを介して第2の端末に送信する手段、

第2の端末から、第1の端末と第2の端末との間の暗号化通信のための鍵情報を含む応答メッセージを第2の暗号化通信チャネルを介して受信し、その応答メッセージを第1の暗号化通信チャネルを介して第1の端末に送信する手段

として機能させるプログラム。

【請求項29】

コンピュータを、ネットワークに接続された第1の端末と第2の端末との間に暗号化通信チャネルを確立するために使用する公開鍵を管理する公開鍵管理装置として機能させるプログラムであって、コンピュータを、

第1の端末との間で暗号化通信のための鍵情報を交換し、第1の端末と相互に認証を行う暗号化通信チャネル確立手段、

第1の端末から、前記暗号化通信チャネル確立手段により確立された公開鍵管理装置と第1の端末との間の暗号化通信チャネルを介して、第1の端末の公開鍵を受信する手段、受信した公開鍵の公開鍵証明書を生成し、当該公開鍵証明書を、公開鍵管理装置と第1の端末との間の前記暗号化通信チャネルを介して第1の端末に送信する手段

として機能させるプログラム。

【請求項30】

コンピュータを、ネットワークに接続された第1の端末と第2の端末との間で暗号化通信チャネルを確立するために使用する公開鍵を管理する公開鍵管理装置として機能させるプログラムであって、コンピュータを、

第1の端末との間で暗号化通信のための鍵情報を交換し、第1の端末と相互に認証を行う第1の暗号化通信チャネル確立手段、

第2の端末との間で暗号化通信のための鍵情報を交換し、第2の端末と相互に認証を行う第2の暗号化通信チャネル確立手段、

第1の端末から、前記第1の暗号化通信チャネル確立手段により確立された公開鍵管理装置と第1の端末との間の第1の暗号化通信チャネルを介して、第1の端末の公開鍵を受信する手段、

受信した公開鍵を記憶装置に格納する手段、

前記第2の暗号化通信チャネル確立手段により確立された公開鍵管理装置と第2の端末との間の第2の暗号化通信チャネルを介して、第1の端末の公開鍵を第2の端末に送信する手段

として機能させるプログラム。

【請求項31】

コンピュータを、ネットワークに接続されたセッション管理装置を用いて他の端末との間で暗号化通信チャネルを確立する端末として機能させるプログラムであって、コンピュータを、

ネットワークに接続されたセッション管理装置との間で暗号化通信のための鍵情報を交換し、セッション管理装置と相互に認証を行い、セッション管理装置との間で暗号化通信チャネルを確立する暗号化通信チャネル確立手段、

前記端末と前記他の端末との間の暗号化通信のための鍵情報を含む前記他の端末への接続要求メッセージを、前記暗号化通信チャネル確立手段により確立された暗号化通信チャネルを介してセッション管理装置に送信し、前記他の端末から、セッション管理装置を介して、前記端末と前記他の端末との間の暗号化通信のための鍵情報を含む応答メッセージを受信する手段

として機能させるプログラム。

【書類名】明細書

【発明の名称】端末間の暗号化通信チャネルを構築する方法及びそのための装置並びにプログラム

【技術分野】

【0001】

本発明は、ネットワーク上の2つの端末間でセキュアなデータチャネルを構築する技術に関するものである。

【背景技術】

【0002】

従来技術において、IPネットワーク上の2つの端末間でデータチャネルを構築しいわゆるピア・ツー・ピアの通信を行うためには、DNSへの名前登録から、セキュリティを確保するためのFW等の設定・管理、証明書の取得等の作業が必要である。また、多数の端末同士の間で相互認証および暗号化されたピア・ツー・ピアの通信を行うためにはそれら全端末の証明書を取得するか、あるいは全端末のID、パスワードを管理することが必要である。

【0003】

このように、従来技術では、IPネットワーク上の2つの端末間でセキュアなデータチャネルを構築するために煩雑な作業が必要である上、オープンなDNSに名前とアドレスが登録されるため、端末が不正なアクセスを受ける恐れがあるという問題がある。

【0004】

また、端末間に仲介サーバを導入し、一方の端末からのデータチャネルを代理で終端し、他方の端末のデータチャネルも代理で終端し、両端末のデータチャネルを仲介サーバ上でマッチングさせることにより、擬似的に2つの端末間のデータチャネルを実現するしくみも提案されている。しかしながら、この方法には、端末同士の全てのデータが仲介サーバを経由するため、仲介サーバに多大な負荷がかかるという問題がある。また、家庭内端末に対するリアルタイムなアクセスができないという問題もある。

【特許文献1】特開2002-208921号公報

【発明の開示】

【発明が解決しようとする課題】

【0005】

本発明は、上記の点に鑑みてなされたものであり、端末間でセキュアなデータチャネルを容易に構築するための技術を提供することを目的とする。

【課題を解決するための手段】

【0006】

上記の課題は、ネットワークに接続された第1の端末と第2の端末との間で暗号化通信チャネルを確立するための方法であって、前記ネットワークに接続されたセッション管理装置と第1の端末との間で相互認証を行い、セッション管理装置と第1の端末との間で第1の暗号化通信チャネルを確立するステップと、セッション管理装置と第2の端末との間で相互認証を行い、セッション管理装置と第2の端末との間で第2の暗号化通信チャネルを確立するステップと、第1の暗号化通信チャネルと第2の暗号化通信チャネルとを介して第1の端末と第2の端末との間で鍵情報を交換するステップとを有する方法により解決できる。

【0007】

本発明によれば、相互認証を行うことにより各端末とセッション管理装置との間で相互信頼の関係が築け、これにより、第1の端末と第2の端末との間では、セッション管理装置を介した簡易なシグナリング手順により、暗号化通信チャネルを確立でき、端末間でセキュアなデータチャネルを容易に構築できる。また、その後の端末間通信はセッション管理装置を介すことなく行うことができるので、従来の問題が解決される。

【0008】

また、上記の課題は、ネットワークに接続された第1の端末と第2の端末との間で暗号

化通信チャネルを確立するための方法であって、前記ネットワークに接続されたセッション管理装置と第1の端末との間で暗号化通信のための鍵情報を交換し、セッション管理装置と第1の端末が相互に認証を行い、セッション管理装置と第1の端末との間で第1の暗号化通信チャネルを確立するステップと、セッション管理装置と第2の端末との間で暗号化通信チャネルを確立するステップと、セッション管理装置と第2の端末が相互に認証を行い、化通信のための鍵情報を交換し、セッション管理装置と第2の端末との間で第2の暗号化通信チャネルを確立するステップと、セッション管理装置と第2の端末との間で第2の暗号化通信チャネルを介してセッション管理装置に送信し、セッション管理装置が、その接続要求メッセージを第1の暗号化通信チャネルを介して第2の暗号化通信チャネルを介して第2の端末に送信するステップと、第2の端末が、前記接続要求メッセージの応答として、第1の端末と第2の端末との間の暗号化通信のための鍵情報を含む応答メッセージを第2の暗号化通信チャネルを介してセッション管理装置に送信し、セッション管理装置が、その応答メッセージを第1の暗号化通信チャネルを介して第1の端末に送信するステップとを有する方法によっても解決できる。

【0009】

上記の方法において、第1の端末とセッション管理装置との間のメッセージ通信、及び第2の端末とセッション管理装置との間のメッセージ通信をSIPに基づき行うことができる。

【0010】

また、第1の端末が、前記第1の暗号化通信チャネルを介して、第1の端末の名前とアドレスをセッション管理装置に登録するステップと、第2の端末が、前記第2の暗号化通信チャネルを介して、第2の端末の名前とアドレスをセッション管理装置に登録するステップとを更に有し、第1の端末から送信される前記接続要求メッセージは第2の端末の名前を含み、前記セッション管理装置は、当該名前から第2の端末のアドレスを取得し、当該アドレス宛に前記接続要求メッセージを送信するようにしてもよい。

【0011】

更に、前記セッション管理装置は、端末間で接続を許可するか否かの情報を保持し、接続要求メッセージを受信した場合に、当該情報を参照して、接続要求元の端末が接続要求が許容されているか否かを判断し、許容されていない場合には、接続を拒否することができる。

【0012】

また、前記第1の端末が第3の端末からのアクセスを受けた後に前記各ステップが実行され、前記各ステップの実行により確立された前記第1の端末と前記第2の端末との間の暗号化通信チャネルを介して、前記第1の端末が前記第2の端末からデータを受信し、当該データを前記第3の端末に送信するようにしてもよい。

【0013】

更に、前記第1の端末が第3の端末からのアクセスを受けた後に、前記第1の暗号化通信チャネル及び前記第2の暗号化通信チャネル確立のためのステップ以降の各ステップが実行され、前記各ステップの実行により確立された前記第1の端末と前記第2の端末との間の暗号化通信チャネルを介して、前記第1の端末が前記第2の端末からデータを受信し、当該データを前記第3の端末に送信するようにしてもよい。

【0014】

また、上記の課題は、ネットワークに接続された第1の端末と第2の端末との間に暗号化通信チャネルを確立するための方法であって、前記ネットワークに接続された公開鍵管理装置と第1の端末との間で暗号化通信のための鍵情報を交換し、公開鍵管理装置と第1の端末が相互に認証を行う暗号化通信チャネル確立ステップと、第1の端末が秘密鍵と公開鍵を生成し、当該公開鍵を、前記暗号化通信チャネル確立ステップにより確立された公開鍵管理装置と第1の端末との間の暗号化通信チャネルを介して公開鍵管理装置に送信するステップと、公開鍵管理装置が、受信した公開鍵の公開鍵証明書を生成し、当該公開鍵のステップと、公開鍵管理装置と第1の端末との間の前記暗号化通信チャネルを介して第1の証明書を、公開鍵管理装置と第1の端末との間の前記暗号化通信チャネルを介して第1の

端末に送信するステップと、第1の端末が、第2の端末に当該公開鍵証明書を配布することにより、第1の端末と第2の端末との間で公開鍵を用いた暗号化通信チャネルを確立するステップとを有する方法によっても解決できる。

【0015】

本発明によれば、従来のように煩雑な手続きを得ることなく、公開鍵ベースの暗号化通信チャネルを確立できる。

【0016】

なお、前記公開鍵管理装置は、前記暗号化通信チャネル確立ステップを実行して第1の端末との間で前記暗号化通信チャネルを確立するサーバと、当該サーバに暗号化通信チャネルを介して接続された公開鍵証明書を生成・管理する機能を有する装置とからなるように構成してもよい。

【0017】

また、第1の端末と公開鍵管理装置との間のメッセージ通信はSIPに基づき行うことができる。

【0018】

また、上記の課題は、ネットワークに接続された第1の端末と第2の端末との間で暗号化通信チャネルを確立するための方法であって、前記ネットワークに接続された公開鍵管理装置と第1の端末との間で暗号化通信のための鍵情報を交換し、公開鍵管理装置と第2の端末が相互に認証を行う第1の暗号化通信チャネル確立ステップと、公開鍵管理装置と第2の端末との間で暗号化通信のための鍵情報を交換し、公開鍵管理装置と第2の端末が相互に認証を行う第2の暗号化通信チャネル確立ステップと、第1の端末が秘密鍵と公開鍵を生成し、当該公開鍵を、前記第1の暗号化通信チャネル確立ステップにより確立された公開鍵管理装置と第1の端末との間の第1の暗号化通信チャネルを介して公開鍵管理装置に送信するステップと、公開鍵管理装置は受信した公開鍵を記憶装置に格納し、第2の端末が、当該公開鍵を、前記第2の暗号化通信チャネル確立ステップにより確立された公開鍵管理装置と第2の端末との間の第2の暗号化通信チャネルを介して取得するステップと、第1の端末と第2の端末との間で当該公開鍵を用いた暗号化通信チャネルを確立するステップとを有する方法によっても解決できる。

【0019】

前記公開鍵管理装置は、第1の端末との間、及び第2の端末との間で暗号化通信チャネルを確立する装置と、当該装置と暗号化通信チャネルを介して接続された公開鍵を管理する機能を有する装置とからなるように構成してもよく、第1の端末と公開鍵管理装置との間のメッセージ通信、及び第2の端末と公開鍵管理装置との間のメッセージ通信をSIPに基づき行うこともできる。

【0020】

また、本発明によれば、上記の方法における処理を行うセッション管理装置、端末、及びプログラムが提供される。

【発明の効果】

【0021】

本発明によれば、端末間でセキュアなデータチャネルを容易に構築できる。また、その後の端末間通信はセッション管理装置を介すことなく行うことができるので、仲介サーバを用いる場合の従来の問題が解決される。

【発明を実施するための最良の形態】

【0022】

以下、本発明の実施の形態を図を参照して説明する。

【0023】

(第1の実施の形態)

まず、図1を用いて本発明の第1の実施の形態の概要について説明する。

【0024】

図1に示すように、端末1と端末2との間にセッション管理サーバ3を設置し、端末1

セッション管理サーバ3－端末2間で、端末1－端末2間のデータチャネル構築のためのシグナリング（信号手順）を実行し、データチャネル構築後はセッション管理サーバ3を介さずに端末間のみでデータ通信を行うというものである。

【0025】

シグナリングにおいては、まず、端末1－セッション管理サーバ3間、セッション管理サーバ3－端末2間の各々で、IPsec等の暗号化通信を行うためのセキュアシグナリングチャネル確立のために、暗号鍵情報の交換、相互認証が行われる。そして、端末1－セッション管理サーバ3間、セッション管理サーバ3－端末2間の各々で確立されたセキュアシグナリングチャネルを介してセッション管理サーバへの名前登録、端末1－端末2間のセキュアデータチャネル確立のためのシグナリングが実行される。

【0026】

端末1－セッション管理サーバ3間、セッション管理サーバ3－端末2間でのセキュアシグナリングチャネル確立におけるシグナリングにより、セッション管理サーバ3と端末1との間、セッション管理サーバ3と端末2との間において相互認証に基づく信頼関係が確立されているため、端末1と端末2との間でも信頼関係が確立されている。すなわち、上記の相互認証により、セッション管理サーバ3を介した信頼のチェーンモデルが構築される。従って、端末1－端末2間のセキュアデータチャネル確立のためのシグナリングでは、簡易な鍵情報の交換手順を用いることができる。

【0027】

次に、端末1－セッション管理サーバ3－端末2間の通信のシーケンスを図2を参照して説明する。

【0028】

図2に示すシーケンスは、端末1、セッション管理サーバ3、端末2がインターネット等のIPネットワークに接続されたシステム構成を前提とするものである。

【0029】

各端末は、セッション管理サーバ3との間でシグナリングを実行するシグナリング機能、セキュアデータチャネルを介してデータ通信を行うための機能、及びデータ通信を利用して所望のサービスを提供するアプリケーションを備えている。

【0030】

また、セッション管理サーバは、シグナリングを各端末との間で実行するシグナリング機能、端末間の接続許可等を制御する接続ポリシー制御機能、各端末を認証するための認証機能、端末の名前からIPアドレスを取得する名前解決機能、及び、認証のために用いるID、パスワードを格納するデータベースや、名前とIPアドレスを対応付けて格納するデータベース等を備えている。また、名前解決機能として一般的のDNSと同等の機能を持たせることもできる。

【0031】

図2に示すように、端末1－端末2間でのセキュアデータチャネル構築にあたり、まず、端末1－セッション管理サーバ3間、端末2－セッション管理サーバ3間の各々でセキュアシグナリングチャネルを構築して、名前の登録を行う。

【0032】

すなわち、端末1－セッション管理サーバ3間でIPsec等の暗号通信で用いる鍵情報（暗号鍵生成用の情報）の交換を行う（ステップ1）。その後、自分のID、パスワードを含む情報を暗号化して相手側に送信することにより、相互に認証を行う（ステップ2）。認証後は、セキュアシグナリングチャネルが確立された状態となり、そのチャネルを用いて、端末1は名前とIPアドレスの登録をセッション管理サーバ3に対して行う（ステップ3）。端末1の通信相手となる端末2とセッション管理サーバ3間でも同様のシーケンスが実行され、端末2の名前とIPアドレスがセッション管理サーバ3に登録される（ステップ4、5、6）。

【0033】

その後、端末1から端末2への接続要求が、セキュアシグナリングチャネルを介して送

信される（ステップ7）。接続要求には、端末2の名前と暗号通信用の鍵情報（暗号鍵生成用の情報）が含まれる。接続要求を受信したセッション管理サーバ3は、端末1からの接続要求に関して、端末1が嘘についていないことをチェックし（発信者詐称チェック）、更に、接続ポリシー制御機能を用いて端末1と端末2の接続が許可されているかをチェックし（ステップ8）、許可されていれば、名前解決機能を用いてデータベースを参照することにより端末2の名前から端末2のIPアドレスを取得し（ステップ9）、セキュアことにより端末2の名前から端末2のIPアドレスを取得し（ステップ9）、セキュア化シグナリングチャネルを介して端末2へ接続要求を転送する（ステップ10）。このとき、端末1のIPアドレスも端末2に送信される。端末1と端末2の接続が許可されていなければ、端末1の接続要求は拒否される。このとき、端末2に関する情報は端末1には全く送信されない。

【0034】

接続要求を受信した端末2は、接続要求に対する応答として、暗号通信用の鍵情報を含む応答メッセージをセキュアシグナリングチャネルを介してセッション管理サーバ3に送信し（ステップ11）、セッション管理サーバ3がその応答メッセージを端末1に送る（ステップ12）。このとき、端末2のIPアドレスも端末1に送信される。

【0035】

この手順により、端末1と端末2との間での暗号化通信が可能となる。すなわち、セキュアデータチャネルが確立され、所望のデータ通信が行われる。

【0036】

ステップ1、2及び4、5を経てセキュアシグナリングチャネルが確立されているということは、端末一セッション管理サーバ間で相互に認証が成功しており、信頼関係が成立しているということである。端末1一セッション管理サーバ3間、及び端末2一セッション管理サーバ3間の各々でこのような関係が成立しているので、端末1と端末2との間も相互に信頼できる関係となることから、ステップ7以降は、一般の暗号化通信で用いられる鍵交換手順より簡略化した手順を用いることが可能となっている。

【0037】

上記のシーケンスを実現する手段として、SIP（session initiation protocol）を拡張したプロトコルを用いることが可能である。すなわち、セッション管理サーバ3をSIPプロキシサーバとして機能させ、SIPのメッセージに上記の手順でやり取りされる情報を含ませる。

【0038】

この場合、セキュアシグナリングチャネルの確立及び名前登録のためにREGISTERメッセージを用い、端末1一端末2間のセキュアデータチャネル確立のためにINVITEメッセージを用いることができる。

【0039】

SIPを用いる場合のシーケンス例を図3に示す。

【0040】

図3に示す例は、セキュアなチャネルで接続された複数のセッション管理サーバを経由してシグナリングを行う場合の例である。なお、セキュアなチャネルで接続された複数のセッション管理サーバをセッション管理装置と称する場合がある。図3に示すシーケンスの構成において、端末1のIPアドレスが2001:1234::10、セッション管理サーバAのIPアドレスが2001:6789::5060、セッション管理サーバBのIPアドレスが2001:abcd::5060、端末2のIPアドレスが2001:cdef::10である。

【0041】

各端末とセッション管理サーバ間では予め互いにID、パスワードを配布しておき、端末とセッション管理サーバの各々は、相手のID、パスワードを自分の記憶装置に格納する。また、セッション管理サーバAとセッション管理サーバBの間は、TLS等のセキュアなチャネルを介して通信を行う。

【0042】

まず、端末1、2は、REGISTERメッセージを用いて、セッション管理サーバとのセキュアチャネルの確立、及び、(SIPに準拠した)名前の登録をセッション管理サーバA、Bに対して行う(ステップ21)(図2のステップ1~6に相当する)。なお、この部分の手順については後により詳細に説明する。

【0043】

続いて、端末1が、暗号通信用の鍵情報(図の例では秘密共有鍵生成用の情報)をSDPパラメータとして記述したINVITEメッセージを、端末2への接続要求として、端末1とセッション管理サーバA間のセキュアシグナリングチャネルを介して送信する(ステップ22)。セッション管理サーバAは、そのINVITEメッセージをセッション管理サーバA、B間のセキュアなチャネルを介してセッション管理サーバBに転送する(ステップ23)。

【0044】

なお、端末1からのINVITEメッセージにはRoute-Securityヘッダが含まれる。Route-Securityヘッダが付加されている場合、そのINVITEメッセージを受信した装置は、Route-Securityヘッダ:[アドレス]で示されているアドレスから当該装置までの経路がセキュアなものであるかどうか(例えばIPsecによる暗号化がなされているかどうか)をチェックし、セキュアなものであればそのRoute-Securityヘッダをそのまま残してメッセージを転送する。また、転送先で経路がセキュアなものであるかどうかチェックを要する場合には、Route-Securityヘッダ:[自分のアドレス]を付加したメッセージをそのまま転送する。応答メッセージには、これまでに付されたRoute-Securityヘッダがそのまま付されており、これにより、メッセージがセキュアな経路を介して転送されたものであることがわかる。すわわち、Route-Securityヘッダにより、経路の安全性を担保する仕組みが提供される。

【0045】

セッション管理サーバBは端末2に、INVITEメッセージを端末2とセッション管理サーバB間のセキュアシグナリングチャネルを介して送信する(ステップ24)。なお、セッション管理サーバA及びセッション管理サーバBにおいて端末2の名前解決がなされている。

【0046】

INVITEメッセージを受信した端末2は、暗号通信用の鍵情報をSDPパラメータとして含む応答メッセージを端末1に向けて送信する(ステップ25)。そして、その応答メッセージは、INVITEメッセージと同じルート上を逆の方向に運ばれ、端末1に送信される(ステップ26、27)。

【0047】

その後、受信確認(ACK)メッセージが端末1から端末2に送信され(ステップ28~30)、端末1と端末2との間の暗号化通信(例えばIPsecによる通信)が可能となる。

【0048】

図3のステップ21におけるREGISTERメッセージのシーケンスは、例えば図4に示す通りである。

【0049】

この場合、まず、暗号通信用(IPsec等)の鍵情報を含むREGISTERメッセージを端末からセッション管理サーバに送信する(ステップ211)。セッション管理サーバはその応答として暗号通信用の鍵情報を含む応答メッセージを端末に返す(ステップ212)。続いて、端末は、セッション管理サーバが端末を認証するための認証用情報を含むREGISTERメッセージをセッション管理サーバに送信する(ステップ213)。セッション管理サーバはその応答として、端末がセッション管理サーバを認証するための認証用情報を含む応答メッセージを端末に送信する(ステップ214)。互いの認証が取れた後、セキュアシグナリングチャネルによる暗号化通信が可能となる。

【0050】

その後は、パケットがセキュアシグナリングチャネルを介して暗号化して送受信されるため、通常のREGISTERメッセージシーケンスにより名前の登録が行われる（ステップ215、216）。

【0051】

なお、上記のシーケンスにおいて、IPsec等の暗号化通信に必要なその他の情報は適宜送受信されているものとする。なお、認証用情報は、ID、パスワード等を含む情報でもよいし、証明書（X.509証明書等）でもよい。また、暗号通信用の鍵情報の交換のために用いるメッセージに認証用情報（証明書）を含めてもよい。

【0052】

次に、シグナリングプロトコルとしてSIPを用いる場合の各装置の機能ブロックを図5を参照して説明する。

【0053】

セッション管理サーバは、呼（メッセージ）の転送のための処理を行うSIPプロキシ、SIPの名前登録を行うSIPレジストラ、ID、パスワード、もしくは証明書等を用いて各端末の認証を行う認証モジュール、IPsec等の暗号化通信を行うための暗号化モジュールを有している。

【0054】

また、各端末は、セキュアデータチャネル上での通信を行う機能部、INVITEメッセージの送受信やREGISTERメッセージの発行等を含むSIPに基づくメッセージセッションを行なうSIP機能部、ID、パスワード、もしくは証明書等を用いてセッション管理サーバの認証を行う認証モジュール、IPsec等の暗号化通信を行うための暗号化モジュールを有している。

【0055】

上記のセッション管理サーバ、各端末の機能は、プログラムにより実現されるものであり、本発明におけるセッション管理装置、端末の各手段は、プログラムと、セッション管理装置、端末のハードウェアとで実現されているものである。また、端末は、CPU、メモリ、ハードディスク等を含む一般的なPC等のコンピュータ、モバイル機器等であり、当該コンピュータ等に上記プログラムをインストールすることにより本実施の形態の端末の機能を実現できる。なお、端末はデジタル家電等でもよい。また、セッション管理サーバは、サーバ等のコンピュータであり、当該サーバに上記プログラムをインストールすることにより本実施の形態のセッション管理サーバの機能を実現できる。

【0056】

上記のように本実施の形態のような構成としたことにより、次のような効果を奏する。

【0057】

まず、端末のアドレスが変更される度にREGISTERメッセージによる名前とIPアドレスの登録を行うので、端末側はいわゆる動的IPアドレス割り当てを用いることができる。また、セッション管理サーバが名前解決を行うことから、従来は必要であったオーブンなDNSへの名前登録が不要となる。また、各端末とセッション管理サーバ間でセキュアなチャネルを構築してシグナリングを行うので、端末側でのFW管理が不要となる。また、セッション管理サーバが各端末のID、パスワードを管理するので、端末側で多数のID、パスワードを管理することが不要となる。また、セッション管理サーバ接続ポートのID、パスワードを管理することが不要となる。また、セッション管理サーバ接続ポート数のID、パスワードを管理することができない相手端末に対しては、名前解決さえ許可しリシート御機能により、接続を許可していない相手端末に対しては、名前解決さえ許可しないので、その端末の存在自体を知られることなく、端末が不正なアクセスを受けないので、その端末の存在自体を知られることなく、端末が不正なアクセスを受ける恐れがなくなる。更に、セキュアシグナリングチャネルを介したシグナリングにより、セキュアデータチャネルに必要なポート番号が伝えられるので、シグナリングが正常に完了しない場合には、外部にはポート番号を知られることがない。また、軽いシグナリングだけが中間サーバ（セッション管理サーバ）を経由し、実際のデータ通信は端末間でピア・ツー・ピアで行われるので、中間サーバの負荷が過大となることはない。

【0058】

また、従来技術においては、多数の端末同士の間で相互認証および暗号化されたピア・

ツー・ピアの通信を行うためにはそれら全端末の証明書を取得するか、あるいは全端末のID、パスワードを管理することが必要であったが、本発明によれば、メンバー同士であれば何の事前セキュリティ設定が不要となる。

【0059】

また、従来技術において、データチャネルの暗号化が不要だったとしても、発番号の信憑性を確保する手段として、PKIを使う方法等しかなかったが、本発明によれば、サービス設定（SIPのID/パスワード設定）だけで発番号の詐称・改竄を防ぐことができる。

【0060】

（第2の実施の形態）

次に、上述したような、各端末とセッション管理サーバとの間でセキュアシグナリングチャネルを確立し、そのセキュアシグナリングチャネルを用いて、SIPメッセージに暗号化通信のために必要な鍵情報を含めて送るというしくみを応用した実施の形態を説明する。

【0061】

S S Lによる暗号通信のように公開鍵ベースの認証技術を用いる場合、認証機関（C A）から発行される公開鍵証明書を用いることが必要であるが、C Aから公開鍵証明書を受けたり、それを定期的に更新することは煩雑であり、公開鍵証明書を用いた公開鍵ベースの認証技術の利用は敬遠される場合が多かった。

【0062】

以下で説明する第2の実施の形態では、各端末とセッション管理サーバとの間に信頼関係が確立されることを利用して、端末から公開鍵を簡易にサーバに登録し、そのサーバから簡易にその公開鍵の公開鍵証明書や公開鍵自身を取得できるようにしている。これにより、端末間で容易に公開鍵ベースの認証技術の利用ができ、S S L等の暗号通信を端末間で容易に行うことができる。

【0063】

図6～図8を用いて、本実施の形態における通信手順について説明する。

【0064】

本実施の形態におけるシステム構成は、公開鍵を配布する側の端末11と、その公開鍵の配布を受けて、端末11と公開鍵ベースの暗号通信を行う端末12と、第1の実施の形態と同様の機能を含むセッション管理サーバ21、セッション管理サーバ22、及び、セッション管理サーバ21、22とセキュアなチャネルで接続された簡易C Aサーバ30を有するものである。また、各端末とセッション管理サーバ間は、第1の実施の形態で説明した方法により、セキュアシグナリングチャネルが確立されている。なお、セッション管理サーバと簡易C Aサーバは1つの装置として構成することもできる。また、セキュアなチャネルで接続された簡易C Aサーバとセッション管理サーバをまとめて公開鍵管理装置と称する場合がある。

【0065】

また、本実施の形態では、各端末、セッション管理サーバ21、22、簡易C A管理サーバ30は、公開鍵証明書の発行を要求するためのP U B L I S Hメッセージ（SIPメッセージ）を送受信する機能を有している。P U B L I S Hメッセージは、そのボディ部に公開鍵、公開鍵証明書等を記述して用いる。

【0066】

図6において、まず、端末11は秘密鍵と公開鍵のペアを作成する（ステップ31）。そして、端末11とセッション管理サーバ21間のセキュアシグナリングチャネル、及びセッション管理サーバと簡易C Aサーバ間のセキュアチャネルを介し、P U B L I S Hメッセージを用いて公開鍵を簡易C Aサーバに登録する（ステップ32）。

【0067】

続いて、図7において、端末11が簡易C Aサーバ30から、セッション管理サーバ21及びセキュアシグナリングチャネルを介して、簡易C Aサーバ30の秘密鍵を用いて作成された公開鍵証明書を取得する（ステップ33）。公開鍵証明書は、例えれば、予め定め

た一定の期間のみ簡易CAサーバ30から発行される。なお、この予め定めた一定の期間が、公開鍵証明書の有効期間と一致する。そして、図8に示すように、端末11は、一般的に、公開鍵証明書を配布することにより（ステップ34）、例えば、端末11との端末13に公開鍵証明書を配布することにより（ステップ34）、例えれば、端末11と端末13間でのSSL通信が可能となる。なお、端末11と端末13間で公開鍵を用いてSSL通信を行う方法は従来のSSL通信の方法と同じである。

【0068】

また、簡易CAサーバ30とセキュアに接続され、簡易CAサーバ30と信頼関係にある端末12は、端末11の公開鍵を公開鍵証明書という形式にせずに簡易CAサーバ30から受信できる（ステップ35）。そして、端末11と端末12間で公開鍵ベースの暗号通信を行うことが可能となる。

【0069】

端末11と端末13間でセキュアデータチャネル（SSL通信チャネル）を構築する場合におけるシーケンスを図9に示す。なお、図9には、セッション管理サーバ22を図示していない。

【0070】

端末11とセッション管理サーバ21において、REGISTERメッセージによりセキュアシグナリングチャネルを確立し、SIP名前登録を行までの手順（ステップ41）は、第1の実施の形態と同じである。また、セッション管理サーバ21と簡易CAサーバ30間はTLSセキュアチャネルにより接続されている。また、端末13は、簡易CAサーバ30自身の公開鍵を予め取得しているものとする。

【0071】

端末11は、端末11の公開鍵を登録するために、まず公開鍵をSIPボディ部に含むPUBLISHメッセージをセッション管理サーバ21に送信する（ステップ42）。セッション管理サーバ21はPUBLISHメッセージを簡易CAサーバ30に転送する（ステップ43）。簡易CAサーバ30は、公開鍵の登録及び公開鍵証明書の発行を行い、（ステップ44）。簡易CAサーバ30は、公開鍵の登録及び公開鍵証明書の発行を行い、（ステップ45）。その後、端末11と端末13間でSSL暗号化通信のためのセッションを開始する（ステップ46～）。ステップ46以降は、従来のSSL通信を行うための手順と同じである。すなわち、ステップ45までの処理を予め行っておくことにより、それ以降の任意のタイミングで端末間のSSL通信を自由に行うことができる。

【0072】

図10に各装置の機能ブロック図を示す。

【0073】

セッション管理サーバの機能は第1の実施の形態と同様である。端末は、図5に示した機能に加えて、SIP機能部内に、PUBLISHメッセージの送信機能を有している。また、秘密鍵、公開鍵の生成機能及び公開鍵証明書の管理機能を有している。また、簡易CAサーバは、暗号化モジュール、認証モジュール、SIP機能部に加えて、公開鍵の管理や公開鍵証明書の発行を行う機能を有している。公開鍵の管理とは、例えれば、公開鍵を理や公開鍵証明書の発行を行う機能を有している。公開鍵の管理とは、例えれば、公開鍵を記憶装置に格納することである。その公開鍵に対応する端末の識別情報とともに記憶装置に格納することである。

【0074】

上記のように、本実施の形態によれば、端末とセッション管理サーバ及び簡易CAサーバとの信頼関係をもとに、簡易な公開鍵管理モデルを実現できる。

【0075】

上記の各実施の形態では、SIPを情報送受信の手段として用いる場合を例にとって説明しているが、情報送受信の手段としてはSIPに限定されるものではない。例えれば、SIPに代えてHTTPを用いることができる。

【0076】

（第3の実施の形態）

セキュアシグナリングチャネルを利用したシグナリングによりセキュアデータチャネルを構築するしくみを応用した更なる実施の形態を次に説明する。なお、以下の説明において、“`http`”は、特に示していない場合には、“`http`”を含む広い意味で使用する。

【0077】

本実施の形態は、図2の構成における一方の端末（例えば端末1）に、`http`からS IPへのプロトコル変換を行うゲートウェイ機能（以下、端末1をゲートウェイ装置1と呼ぶ）を備え、携帯電話、PDA等のモバイル端末がゲートウェイ装置1にアクセスすることにより、モバイル端末と端末2間でのセキュアなデータチャネルによる通信を可能とする形態である。

【0078】

図11に、本実施の形態の全体構成を示す。図11に示すように、図2に示す構成における端末1をゲートウェイ装置1に置き換え、モバイル端末41や、社内のファイアウォール配下にあるWebブラウザ端末42等がゲートウェイ装置1にアクセスし、ゲートウェイ装置1と端末2間でセキュアデータチャネルが構築され、ゲートウェイ装置1を介してモバイル端末41等と端末2間で通信を行う。なお、端末2は、例えば特定のユーザからのアクセスのみを許容するWebサーバである。

【0079】

次に、図12のシーケンスチャートを参照して、本実施の形態の動作を説明する。なお、図12のシーケンスにおいて、ゲートウェイ装置1とセッション管理サーバ3間、及びセッション管理サーバ3と端末2間におけるセキュアシグナリングチャネルは構築済みであるものとする。以下、ゲートウェイ装置1にアクセスする端末として、モバイル端末41を例にとり説明する。

【0080】

まず、モバイル端末41が`http`プロトコルを用いてゲートウェイ装置1にアクセスする（ステップ51）。アクセスの際、ゲートウェイ装置1は、モバイル端末41の電話番号を取得する。また、モバイル端末41からゲートウェイ装置1に、IDとパスワードを送信するようにしてもよい。ゲートウェイ装置1は、電話番号、もしくはID、パスワードによりモバイル端末41の認証を行う（ステップ52）。

【0081】

ゲートウェイ装置1は、図13に示すような、ユーザ識別子（電話番号やID）と、そのユーザに接続許容されている接続先の名前を格納するテーブルを保持している。例えば、ゲートウェイ装置1は、モバイル端末41からのアクセスを受けて、当該テーブルから、名前を取得し、モバイル端末41にそれを送信する。モバイル端末41では、その名前を表示し、ユーザに特定の名前を選択させ、選択された名前をゲートウェイ装置1に送信する。これにより、ゲートウェイ装置1は、モバイル端末41のアクセス先の名前を取得する。このような方法に代えて、モバイル端末41から直接名前を入力してゲートウェイ装置1に送信するようにしてもよい。また、モバイル端末41で表示するものを、名前そのものではなくその名前に対応したサイトの概要を示す画像としてもよい。

【0082】

上記のようにして名前を取得したゲートウェイ装置1は、その名前を含むINVITEメッセージをセッション管理サーバ3に送信することにより、その名前が示す接続先（本実施の形態では端末2）への接続要求を行う。図12に示すステップ53～56の処理は、図2のステップ7～12に示す処理と同じである。

【0083】

セキュアデータチャネル確立の後、ステップ59において、モバイル端末41に`http`レスポンスが返される。その後、モバイル端末41とゲートウェイ装置1との間、及びゲートウェイ装置1と端末2との間で`http`プロトコル、もしくは`https`プロトコル等による通信が行われる。ここでは、ゲートウェイ装置1が端末2からデータを受け、それをモバイル端末41に送信する動作を行う。また、必要に応じて、モバイル端末41

への表示に適するように、ゲートウェイ装置1にてデータ変換が行われる。また、モバイル端末41からのリクエストをゲートウェイ装置1が受け、それを端末2に送信している。

【0084】

上記の例ではゲートウェイ装置1とセッション管理サーバ3間に共通のセキュアシグナリングチャネルが予め構築されているものとしたが、モバイル端末41によるアクセスに応じて、当該モバイル端末41用に、ゲートウェイ装置1とセッション管理サーバ3間にセキュアシグナリングチャネルを設けてもよい。

【0085】

図14に、ゲートウェイ装置1の機能ブロック図を示す。なお、図14は、データチャネル構築のためのシグナリングをするための機能を主に示している。

【0086】

図14に示すように、ゲートウェイ装置1は、httpプロトコル処理を行うWebサーバ部51、擬似SIP機能部52、SIP制御部53、IPsec制御部54、モバイル端末の認証等のために用いるデータベース55を備えている。また、図示していないが、セキュアデータチャネル確立後にゲートウェイ装置1と端末2間でhttp通信を行うためのhttpプロトコル処理部を備えている。

【0087】

擬似SIP機能部52は、擬似SIP機能制御部521を有しており、モバイル端末41からのアクセスに応じて個別擬似SIP機能部522を生成する。個別擬似SIP機能部522は、アクセスしてきたモバイル端末に代わって、セキュアシグナリングデータチャネル確立のためのシグナリングを行うためのものである。擬似SIP機能部52は、モバイル端末に代わって擬似的に、図2等に示した端末におけるSIP機能部としての役割を果たすことから、“擬似”SIP機能部と称している。個別擬似SIP機能部522では、SIPメッセージに含める実質的な情報を生成してSIP制御部53に渡し、SIP制御部53がSIPプロトコルに従ったパケットを生成して、送信している。IPsec制御部54は、図5に示す暗号化モジュールに相当する。

【0088】

次に全体の動作を説明する。なお、ゲートウェイ装置1とセッション管理サーバ3間ににおけるセキュアシグナリングチャネルの構築は、SIP制御部53により既に行われているものとする。なお、モバイル端末とゲートウェイ装置間の通信はhttp、httpsのいずれでもよい。

【0089】

まず、モバイル端末41からのhttpリクエストをWebサーバ部51が受信する。Webサーバ部51は、httpリクエストの情報を擬似SIP機能制御部521に渡す。擬似SIP機能制御部521は、その情報に含まれるID等の情報を用い、データベース55を参照することによりアクセスしてきたモバイル端末41の認証を行う。認証がOKであれば、アクセスしてきたモバイル端末41に対応する個別擬似SIP機能部522を生成する。そして、例えば前述したような接続先名前取得手順により、モバイル端末41のユーザが希望する接続先の名前を取得する。なお、図13に示すテーブル情報はデータベース55に含まれる。

【0090】

その後、個別擬似SIP機能部522は、接続要求となるINVITEメッセージを成し、SIP制御部53を介してセッション管理サーバ3に送信する。そして、図12に示すシーケンスにより、IPsec制御部54が、端末2との間でのIPsecコネクション（セキュアデータチャネル）を作成する。これにより、これ以後、セキュアデータチャネルを介してゲートウェイ装置1と端末2との間で、例えばhttpもしくはhttpsによる通信を行うことができる。そして、ゲートウェイ装置1が受信したデータは、必要に応じて変換されてモバイル端末41に送信される。

【0091】

以上説明したように、本実施の形態によれば、ゲートウェイ装置1が、モバイル端末4₁等の代わりとしての擬似SIP機能を備え、モバイル端末4₁の代わりにセキュアデータチャネル構築のためのシグナリングを行う。

【0092】

従って、http通信のみの機能を持つ端末でも、接続相手側がSIPに基づく通信によりチャネルを確立する端末であることを全く意識せずに、従来のhttp接続をゲートウェイ装置1に対して行うだけで、接続相手の端末とセキュアデータチャネルを用いたセキュアな通信を行うことが可能となり、第1の実施の形態で説明したしきみの適用範囲がより広くなる。

【0093】

また、ゲートウェイ装置1に、各端末が接続可能な相手先を格納した図13に示すようなテーブルを保持することにより、携帯電話などの操作系が貧弱な端末でも、ゲートウェイのポータルサイトにアクセスして相手先を選択するだけで、相手方への簡易な接続が可能となる。

【0094】

本発明は、上記の実施例に限定されることなく、特許請求の範囲内で種々変更・応用が可能である。

【図面の簡単な説明】

【0095】

【図1】本発明の第1の実施の形態の概要について説明するための図である。

【図2】端末1—セッション管理サーバ3—端末2間の通信のシーケンス図である。

【図3】シーケンスを詳細に示す図である。

【図4】REGISTERメッセージのシーケンスを示す図である。

【図5】シグナリングプロトコルとしてSIPを用いる場合の各装置の機能ブロック図である。

【図6】第2の実施の形態における通信手順を説明するための図である。

【図7】第2の実施の形態における通信手順を説明するための図である。

【図8】第2の実施の形態における通信手順を説明するための図である。

【図9】端末1₁と端末1₃間でセキュアデータチャネル（SSL通信チャネル）を構築する場合におけるシーケンス図である。

【図10】第2の実施の形態における各装置の機能ブロック図である。

【図11】第3の実施の形態におけるシステム構成図である。

【図12】第3の実施の形態の動作を示すシーケンスチャートである。

【図13】ユーザと接続先の対応を示すテーブルである。

【図14】ゲートウェイ装置1の機能ブロック図である。

【符号の説明】

【0096】

1、2、11、12、13 端末

3、A、B、21、22 セッション管理サーバ

30 簡易CAサーバ

41 モバイル端末

42 FW配下Webブラウザ端末

51 Webサーバ部

52 擬似SIP機能部

53 SIP制御部

54 IPsec制御部

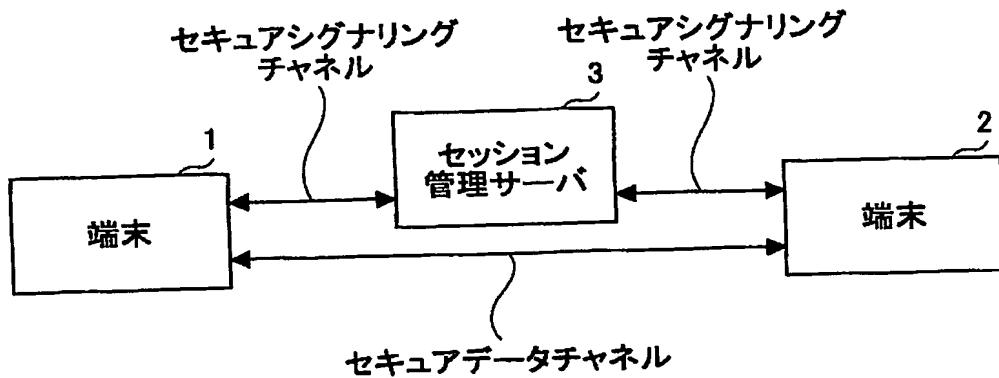
55 データベース

521 擬似SIP機能制御部

522 個別擬似SIP機能部

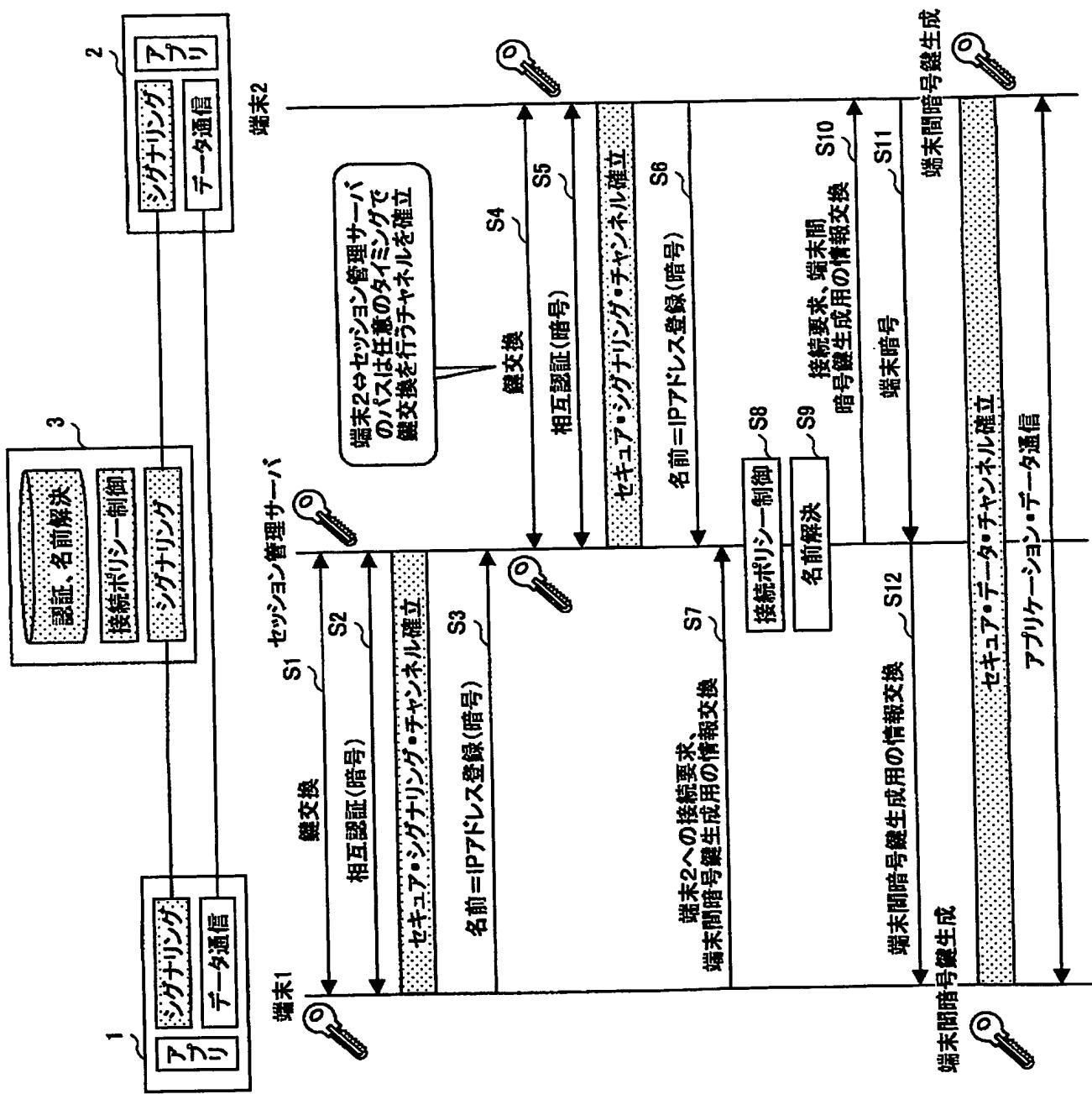
【書類名】 図面
【図 1】

本発明の第1の実施の形態の概要について説明するための図



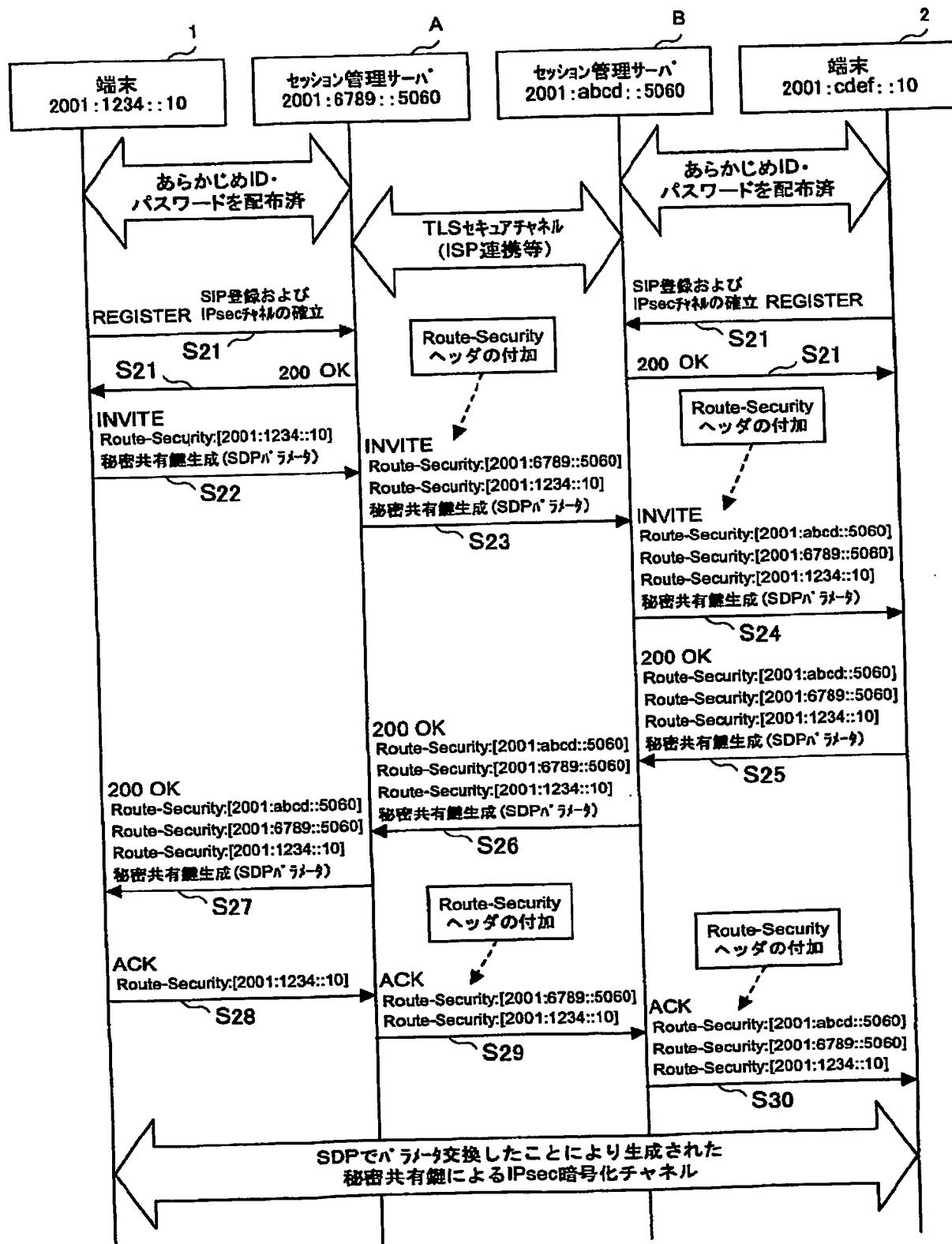
【図2】

端末1—セッション管理サーバ3—端末2間の通信のシーケンス図



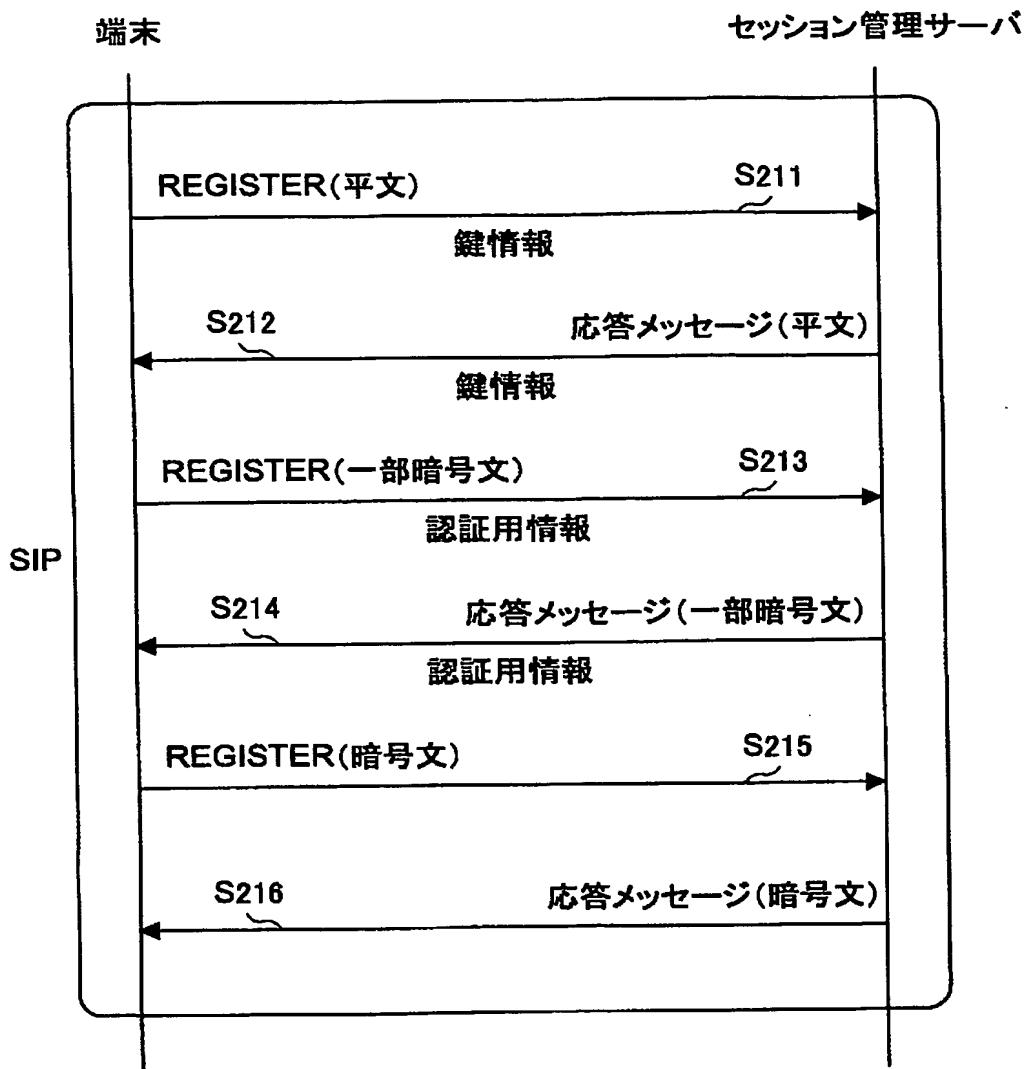
【図3】

シーケンスを詳細に示す図



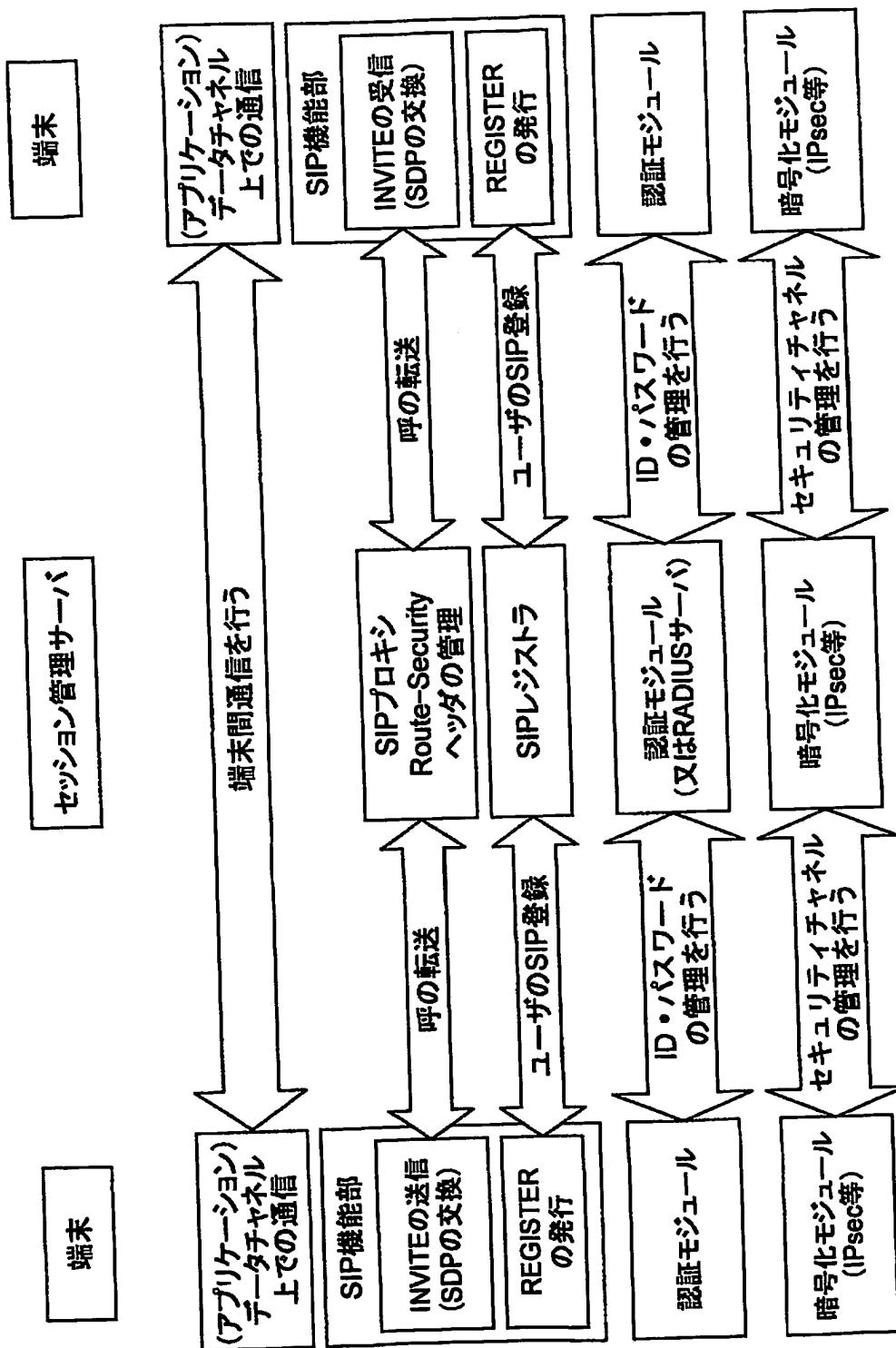
【図4】

REGISTERメッセージのシーケンスを示す図



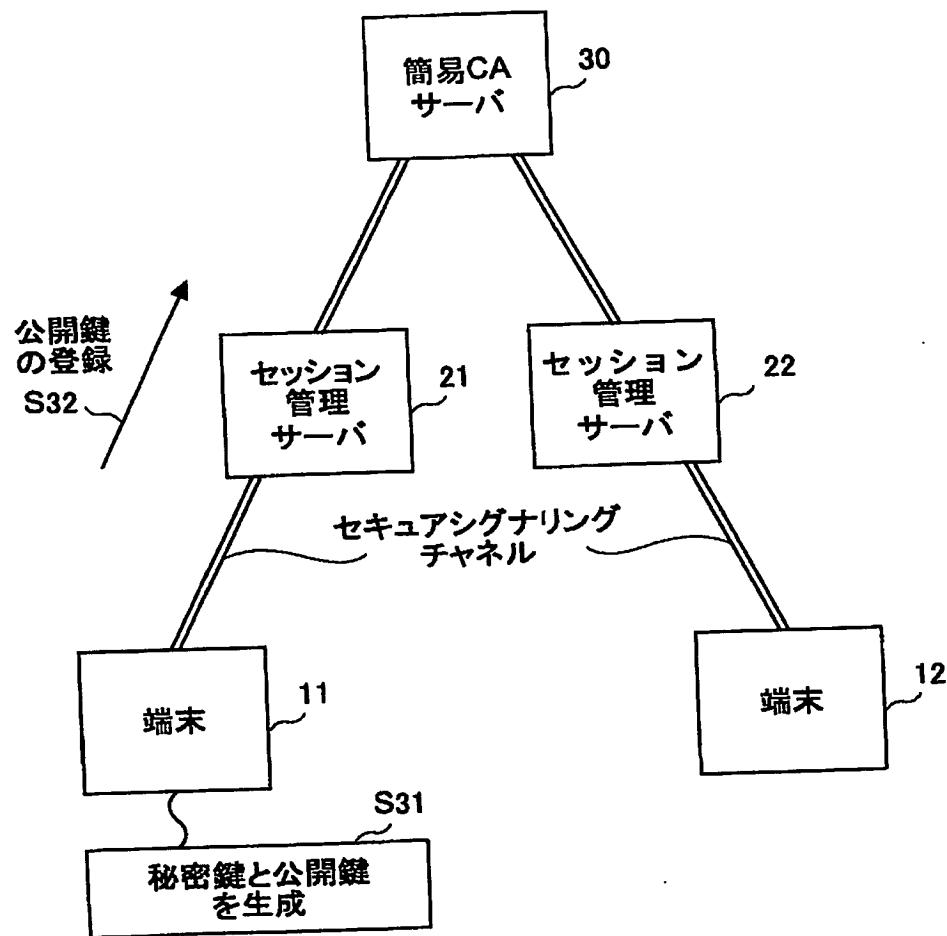
【図5】

シグナリングプロトコルとしてSIPを用いる場合の各装置の機能ブロック図



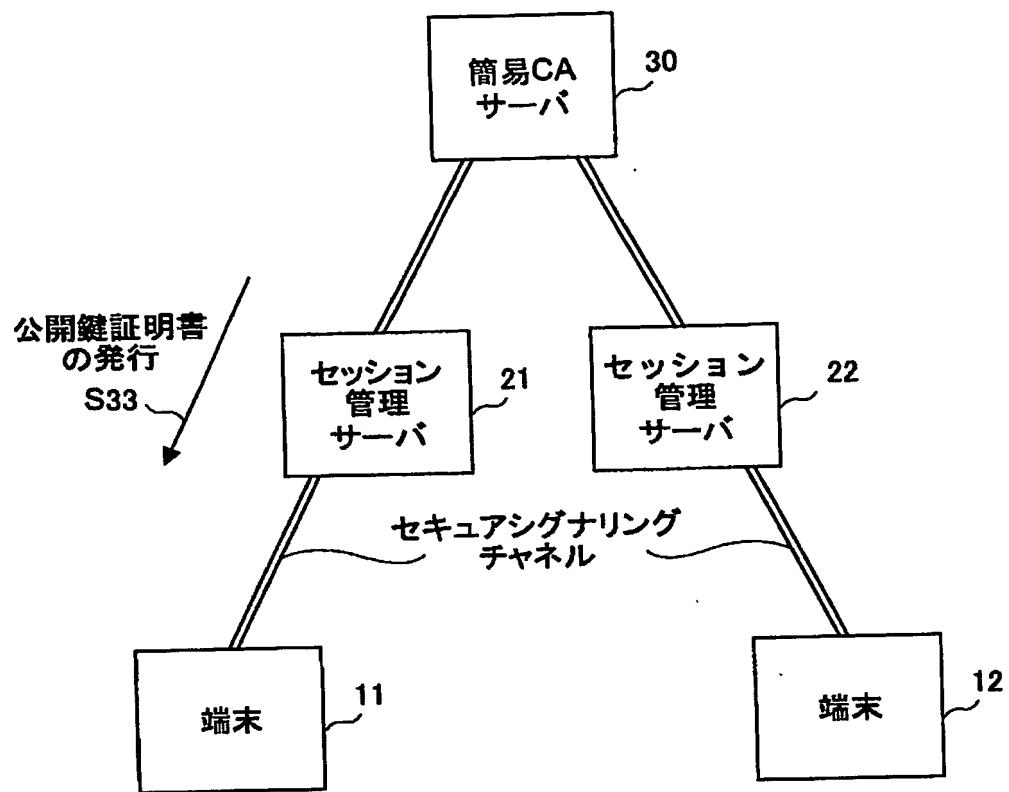
【図6】

第2の実施の形態における通信手順を説明するための図



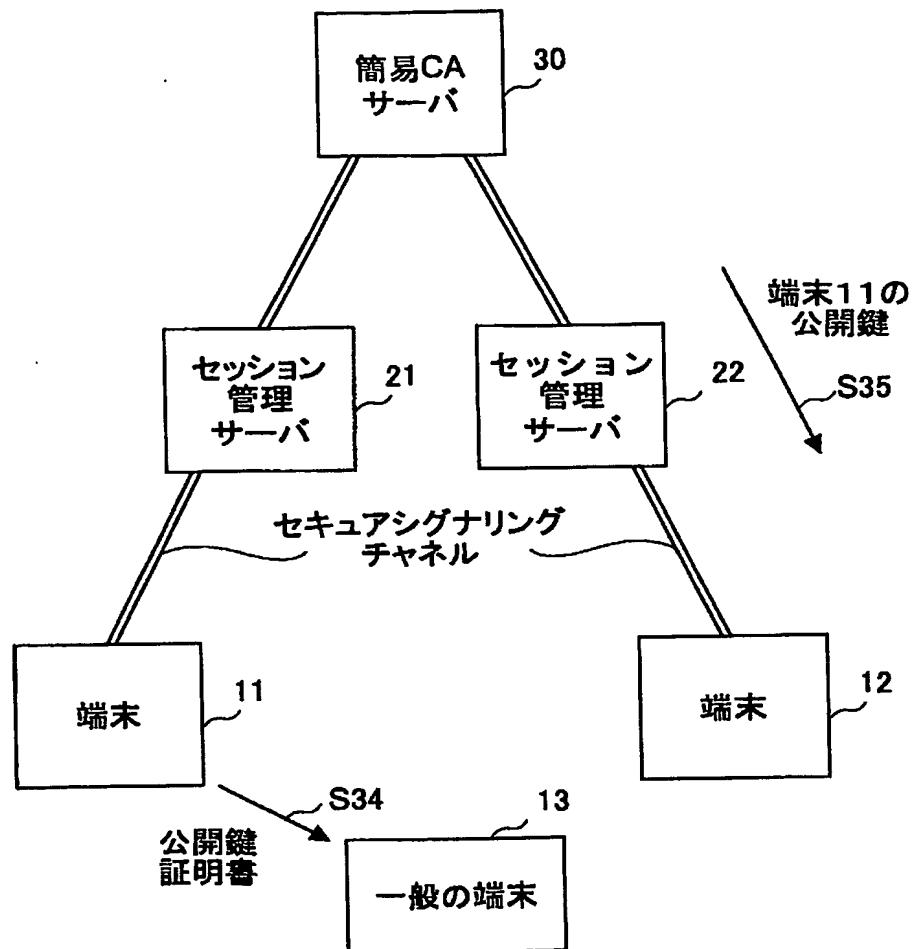
【図7】

第2の実施の形態における通信手順を説明するための図



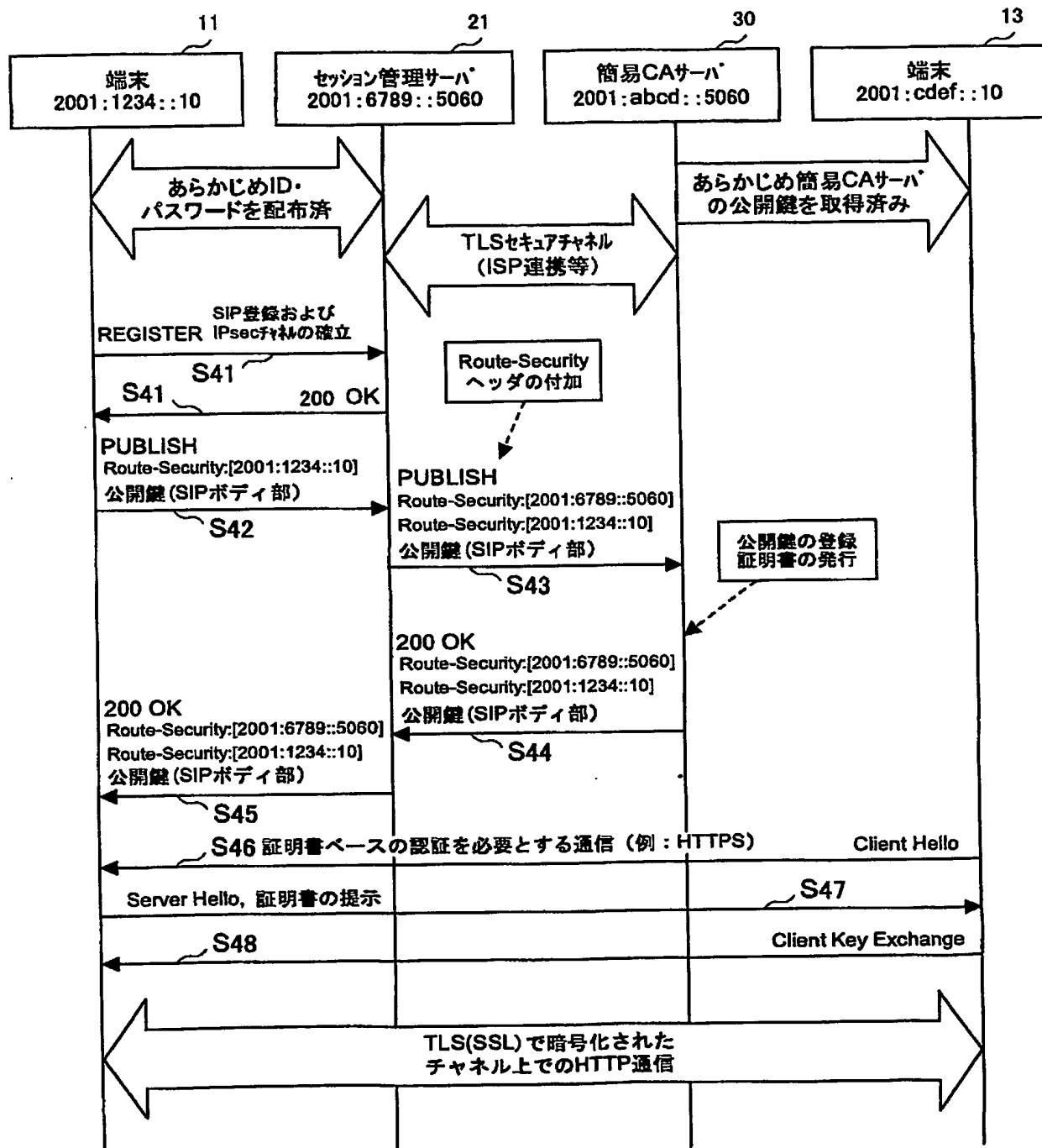
【図8】

第2の実施の形態における通信手順を説明するための図



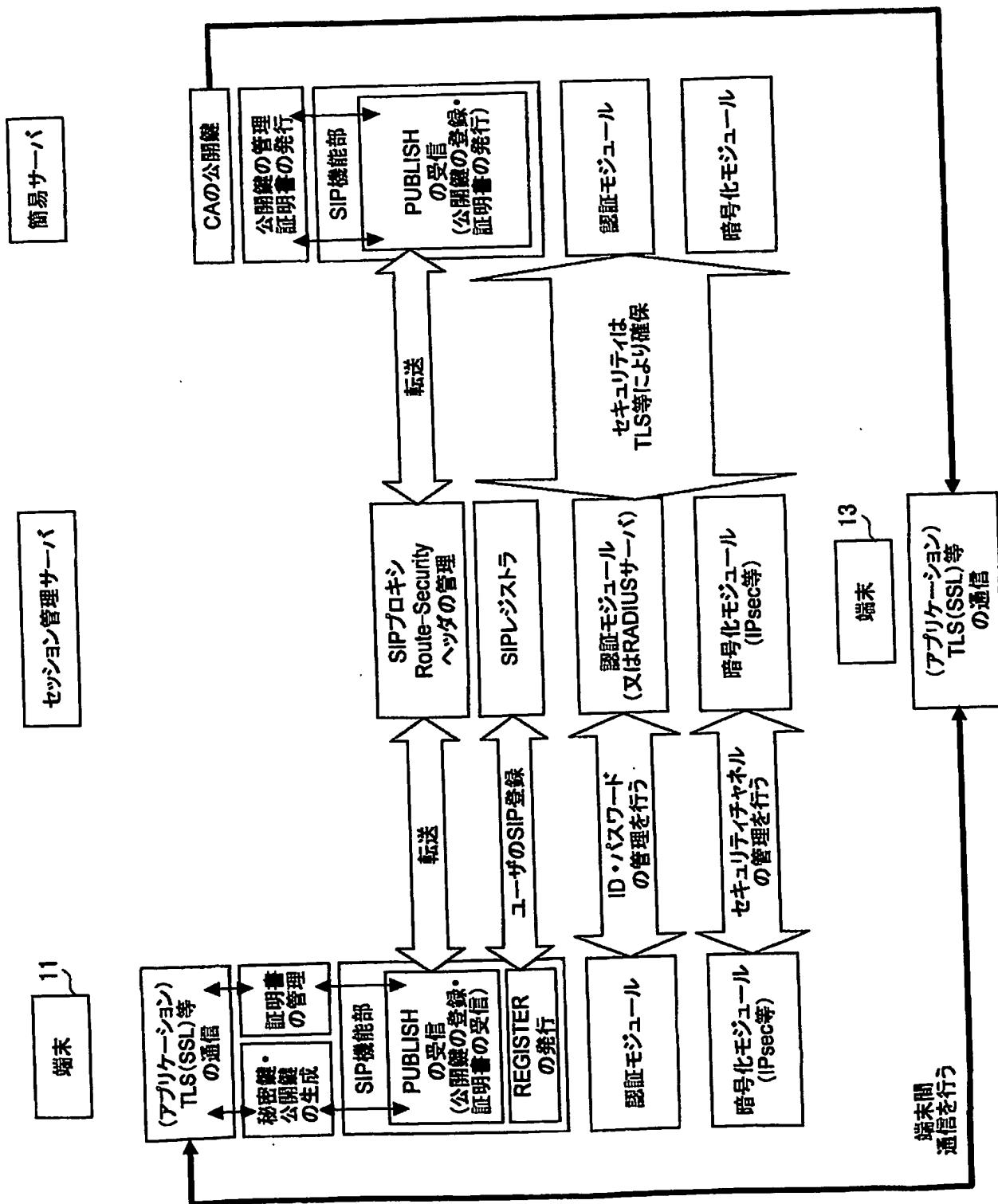
【図9】

端末11と端末13間でセキュアデータチャネル(SSL通信チャネル)を構築する場合におけるシーケンス図



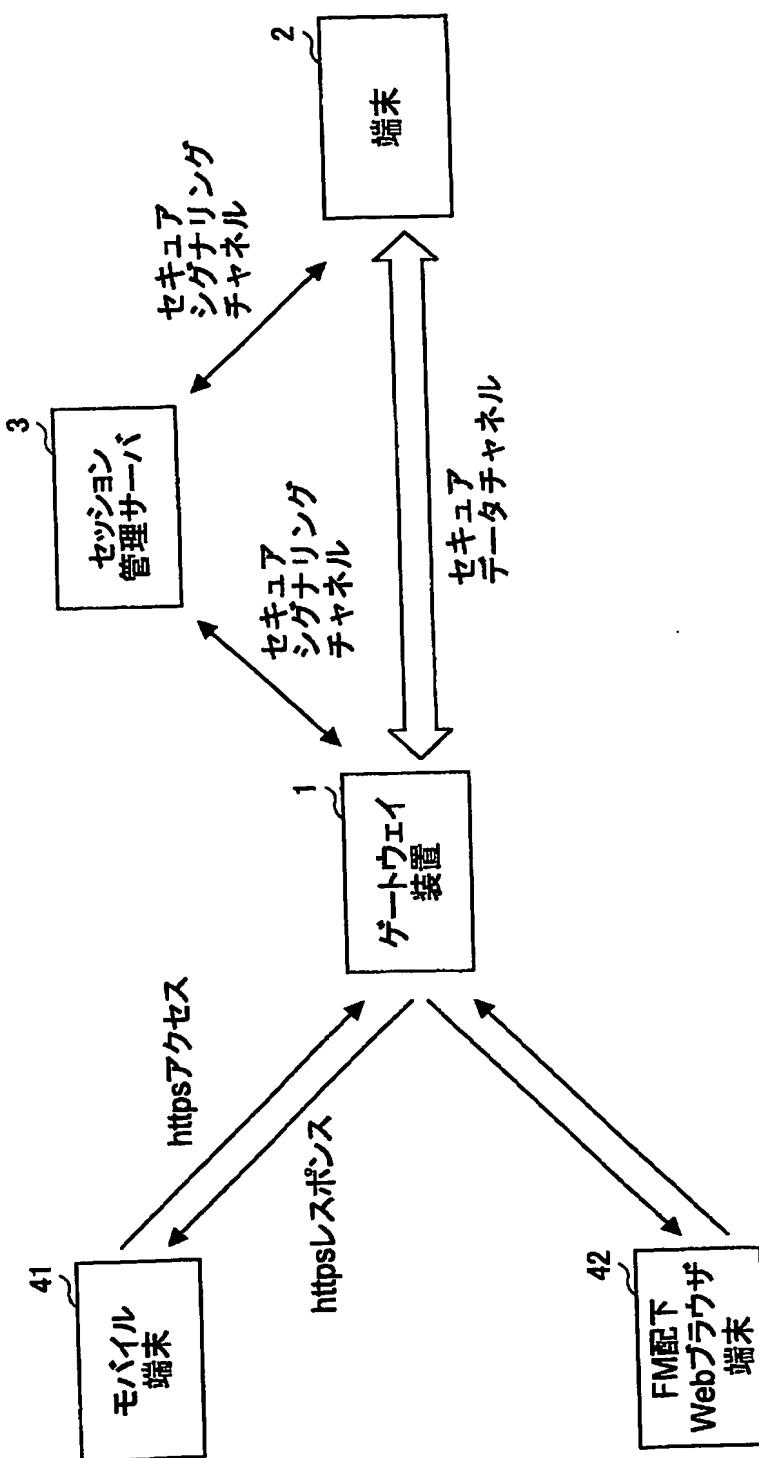
【図10】

第2の実施の形態における各装置の機能ブロック図



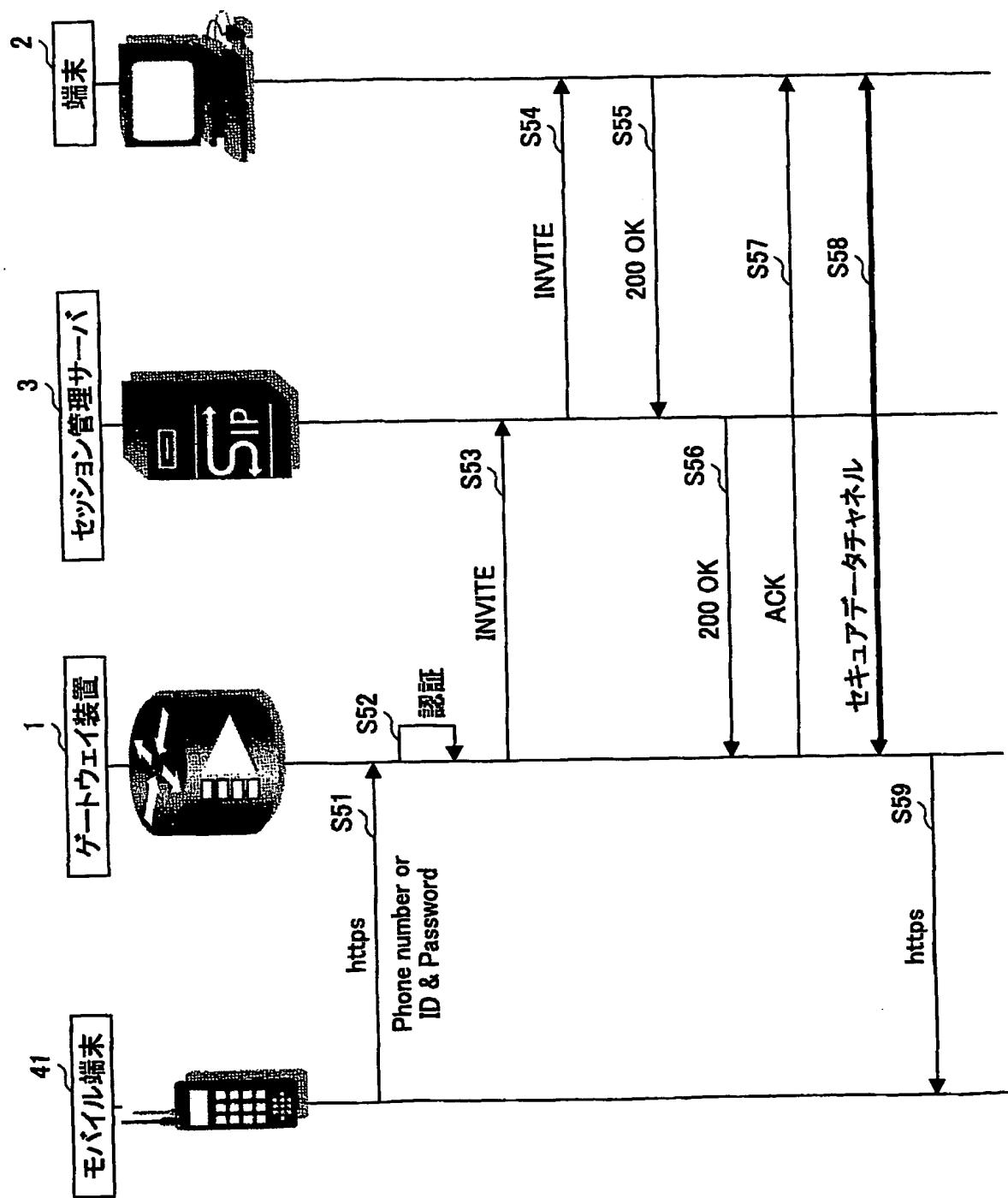
【図 11】

第3の実施の形態におけるシステム構成図



【図12】

第3の実施の形態の動作を示すシーケンスチャート



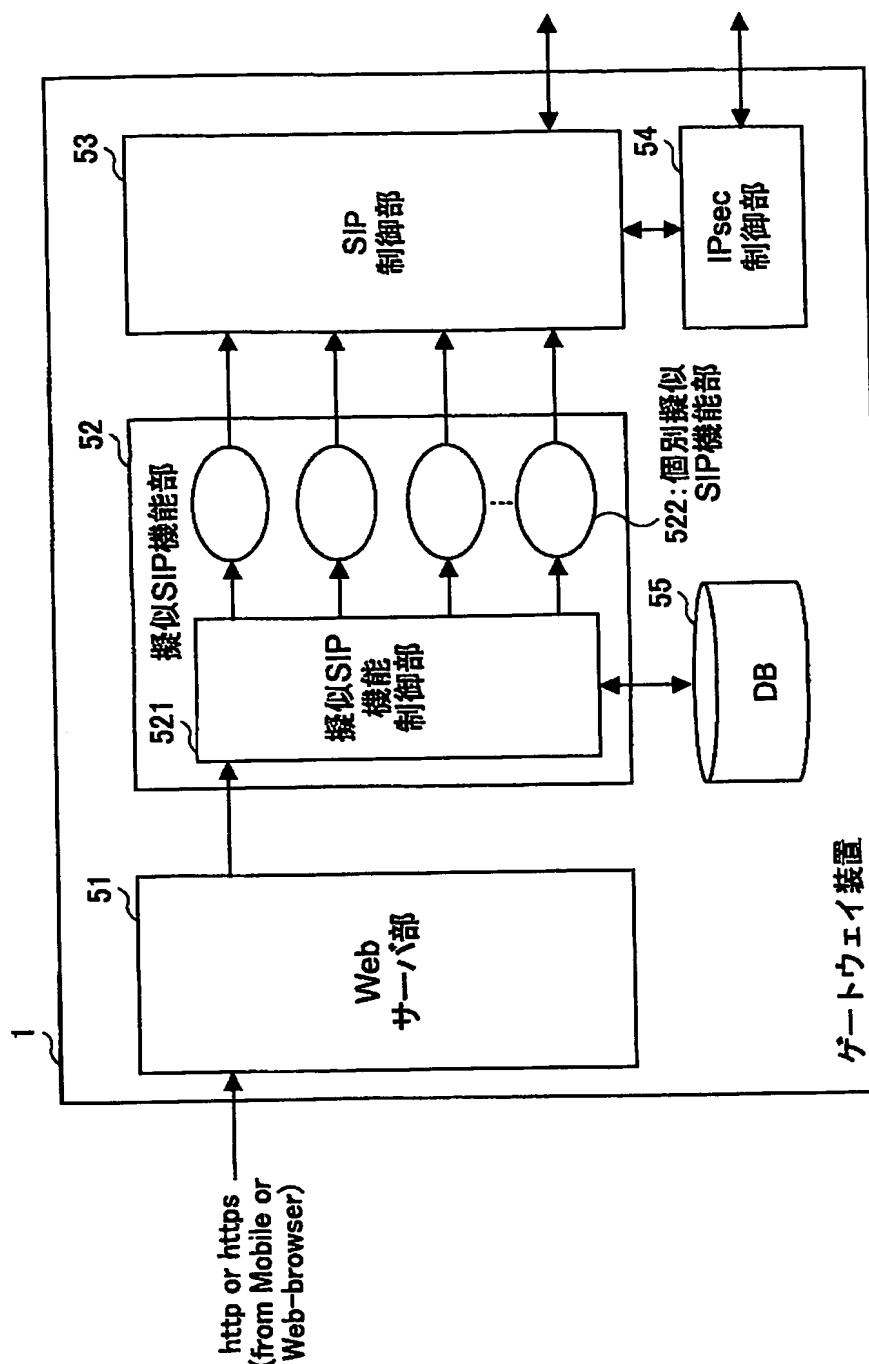
【図13】

ユーザと接続先の対応を示すテーブル

ユーザ識別子	アクセス先の名前
× × ×	AAA,BBB,CCC,.....
⋮	⋮

【図14】

ゲートウェイ装置1の機能ブロック図



【書類名】要約書

【要約】

【課題】 端末間でセキュアなデータチャネルを容易に構築するための技術を提供する。

【解決手段】 ネットワークに接続された第1の端末と第2の端末との間で暗号化通信チャネルを確立するための方法において、前記ネットワークに接続されたセッション管理装置と第1の端末との間で相互認証を行い、セッション管理装置と第1の端末との間で第1の暗号化通信チャネルを確立し、セッション管理装置と第2の端末との間で相互認証を行い、セッション管理装置と第2の端末との間で第2の暗号化通信チャネルを確立し、第1の暗号化通信チャネルと第2の暗号化通信チャネルとを介して第1の端末と第2の端末との間で鍵情報を交換する。

【選択図】 図1

特願2004-034172

出願人履歴情報

識別番号 [399035766]

1. 変更年月日 1999年 6月 9日

[変更理由] 新規登録

住所 東京都千代田区内幸町一丁目1番6号
氏名 エヌ・ティ・ティ・コミュニケーションズ株式会社

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record.**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

BLACK BORDERS

- IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
 - FADED TEXT OR DRAWING**
 - BLURRED OR ILLEGIBLE TEXT OR DRAWING**
 - SKEWED/SLANTED IMAGES**
 - COLOR OR BLACK AND WHITE PHOTOGRAPHS**
 - GRAY SCALE DOCUMENTS**
- LINES OR MARKS ON ORIGINAL DOCUMENT**
- REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**

OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.